The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
12/14/2011

SUBJECT:
Multiple Vulnerabilities in Oracle JRE Java Platform

OVERVIEW:
Multiple vulnerabilities have been discovered in the Oracle Java (formerly known as Sun Java) Runtime Environment (JRE) that could impede proper operations. The Java Runtime Environment is used to enhance the user experience when visiting web sites and is installed on most desktops and servers. These vulnerabilities may be exploited if a user visits or is redirected to a specifically crafted web page, or opens a specially crafted file.

Please note that this update is not part of the Oracle Quarterly Critical Patch Update. The last quarter update was in October 2011. The next update is scheduled for January 10, 2012.

SYSTEMS AFFECTED:
- Oracle Java JRE 1.6.0_29
- Oracle Java JRE 1.5.0_32
- Oracle Java JRE 1.4.2_35

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in the Oracle Java (formerly known as Sun Java) Runtime Environment (JRE) that could impede proper operations.

Many bugs/vulnerabilities were fixed in this Oracle Java JRE release; the most notable was the vulnerability impacting the establishing of TLS/SSL connections. The previous release of Oracle Java JRE introduced a bug that prevented the proper establishing of TLS/SSL connection when certain parameters were used; as of this writing, the only connections using TLS_DH_anon_WITH_AES_128_CBC_SHA has been confirmed. This resulted in applications hanging due to Java incorrectly throwing an IndexOutOfBoundsException or sending an unexpected extra TLS/SSL packet in communications between server and client.

RECOMMENDATIONS:
The following actions should be taken:
- Upgrade to the latest Oracle Java JRE version supported on your platform.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails, IM (Instant Messages) or attachments especially from un-trusted sources.

REFERENCES:

Oracle:

http://www.oracle.com/technetwork/java/javase/6u30-relnotes-1394870.html
http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7103725
http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7105007
http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6761678
http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6670868
http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7041800
http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6682380